

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) In a personal computer, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:
storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer;
retrieving ~~the an~~ identification code from ~~the a non-erasable memory location~~ in said personal computer;
generating a cryptographic key derived at least in part from said identification code;
encrypting data for storage on one of said data storage media using said cryptographic key.
2. (Original) The method of Claim 1, additionally comprising:
retrieving information from a memory location; and
disabling encryption of data routed to one of said data storage media in response to said information.
3. (Original) The method of Claim 1, wherein said retrieving is performed without intervention by a host processor.
4. (Original) The method of Claim 3, additionally comprising verifying said key, wherein said verifying occurs without intervention of said host processor.
5. (Currently Amended) A method of making a computer comprising:
storing a hardware identifier in a non-erasable memory integrated circuit at the time of manufacture of the computer, wherein the hardware identifier is defined at least in part by information associated with components of said computer;
installing said memory integrated circuit into said computer;
providing a data path to data storage media;
coupling a logic circuit comprising an encryption engine to said data path; and
connecting said memory integrated circuit to said logic circuit.
6. (Original) The method of Claim 5, wherein said act of connecting comprises routing a serial data bus from said memory integrated circuit to said logic circuit.

Appl. No. : 09/277,335
Filed : March 26, 1999

7. (Currently Amended) In a computer system comprising host computing logic and at least one data storage device, a method of data storage comprising encrypting user generated data with an encryption process, wherein said encryption process is defined at least in part with information assigned to and associated with said host computing logic, wherein said information is stored in a non-erasable memory in said computer system during manufacture of said computer system.

8. (Previously Amended) The method of Claim 7, wherein said information is permanently associated with said host computing logic.

9. (Original) The method of Claim 7, wherein said information comprises a multi-bit identification code.

10. (Original) The method of Claim 9, additionally comprising the act of deriving an encryption key at least in part from said identification code.

11. Cancelled

12. (Original) The method of Claim 7, additionally comprising defining said encryption process at least in part from user input to said computer system.

13. (Previously Added) The method of Claim 1, wherein encrypting data for storage is performed on an encrypting device that is positioned in a data path between a central processing unit and the data storage medium.

14. (Previously Added) The method of Claim 1, wherein all data that is transmitted to the data storage media is encrypted.